LATHAM & WATKINS LLP
Andrew B. Clubok (pro hac vice)
andrew.clubok@lw.com
555 Eleventh Street NW, Suite 1000
Washington, D.C. 20004
Telephone: 202.637.2200

Melanie M. Blunschi (SBN 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (SBN 304635)
kristin.whitehead@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111
Telephone: (415) 395-5942

Michele D. Johnson (SBN 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: (714) 540-1235

Counsel for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)

[Additional Counsel Listed Below]

GIBSON, DUNN & CRUTCHER LLP
Christopher Chorba (SBN 216692)
CChorba@gibsondunn.com
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: 213.229.7503

Elizabeth K. McCloskey (SBN 268184)
EMcCloskey@gibsondunn.com
Abigail A. Barrera (SBN 301746)
ABarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

ERICA FRASCO, et al., individually and on behalf of all others similarly situated,

Plaintiffs,

v.

FLO HEALTH, INC., et al.,

Defendants.

Case No. 3:21-CV-00757-JD (consolidated)

DEFENDANT META PLATFORMS, INC.'S TRIAL BRIEF

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

I. INTRODUCTION

As this Court recognized, "[t]here is nothing unjust about using an SDK." Dkt. 154 at 10:2-3. Meta freely offered the Facebook SDK code to app developers for them to use for a variety of purposes, such as improving overall app functionality or helping them advertise to their users. But app developers could use code from the Facebook SDK only if they agreed to abide by Meta's Business Tools Terms, which prohibit developers from sending Meta health or other sensitive information and require developers to have all necessary rights and permissions from their users to send information to Meta.

Hundreds of thousands of app developers agreed to those terms and used the Facebook SDK code to improve their apps. Flo was one of those developers. After agreeing to Meta's terms, Flo chose to integrate code from the Facebook SDK into the Flo Period & Ovulation Tracker App by customizing the publicly available code to send limited information about the app's users to Meta, all without any involvement from Meta. Plaintiffs claim the data Flo shared with Meta included the twelve "Custom App Events" that are at issue in this case. The Custom App Events are customized strings of coded data, and Flo never sent Meta a key for decoding them, so Meta did not know the true meaning behind the limited data that it received, and certainly was not privy to Flo users' conversations with the Flo App. That is typical. Meta does not need to know the meaning of the data it receives to help app developers improve their apps or advertise. Meta relies on app developers like Flo—who are best positioned to notify their users that they are sharing data with Meta, get any necessary permissions from their users, and ensure they are not sending health or other sensitive information—to make sure any data they send complies with Meta's terms.

Despite all this, Plaintiffs seek billions of dollars in statutory damages from Meta. Their lone remaining claim against Meta, which they assert under Section 632 of the California Invasion of Privacy Act ("CIPA"), alleges that Meta used the Facebook SDK to "eavesdrop" on the limited information they and other California-based Flo App users entered into the app during the app's initial onboarding process. Plaintiffs will not be able to prove that theory at trial for at least five reasons:

First, Plaintiffs must prove Meta eavesdropped on their conversations with the Flo App while those conversations were ongoing. But the complained-of conduct is the Flo App sending *different* communications to Meta *after* Plaintiffs completed their communications with the Flo App. The

evidence will show there were two different communications at different times between two different sets of parties—the first between Plaintiffs and the Flo App, and the second between the Flo App and Meta. Meta's receipt of the second communication does not show it eavesdropped on the first, which requires proof that Meta listened in on Plaintiffs' communications with the Flo App while those communications were happening.

Second, under CIPA, Meta cannot be held liable for "eavesdropping" on communications to which it is a party—i.e., the coded Custom App Events that Flo subsequently sent to Meta.

Third, Plaintiffs cannot prove that any party to the alleged communications did not consent to Meta's receipt of the Custom App Event data. Plaintiffs consented by agreeing to Meta's policies that stated Meta "collect[s] information when you . . . use third-party . . . apps that use [Meta's] services." Dkt. 527-3 at 39. And Flo consented by configuring and sending the data to Meta in the first place.

Fourth, Plaintiffs must also prove that Meta intended to receive their health information, but the evidence will show Meta never wanted that information in the first place, and, in fact, expressly forbade Flo and other app developers from sending it that information.

Fifth, Plaintiffs must prove the challenged communications were confidential, but the evidence will show that they knew their communications were being recorded by Flo and that they consented to the alleged data sharing (in some cases even sharing similar information publicly on social media).

Even if Plaintiffs could overcome all these hurdles, their claim would still be barred by the one-year statute of limitations. Plaintiffs' claimed injuries occurred well before June 7, 2020 (i.e., a year before they sued Meta), because they all began using the Flo App before then. And they will not be able to prove that the discovery rule extended their time to file suit because many sources, including Meta's policies and news articles, should have put them on notice of their claim by spring 2019.

Even if Plaintiffs could prove liability, an award of statutory damages would not be appropriate. The Court should not award statutory damages because, among other things, Meta never wanted Plaintiffs' health information, Plaintiffs have not suffered any actual harm from the alleged data sharing, and any privacy intrusion would have been minimal given the limited data shared. And anything approaching a maximum classwide statutory damages award—a number in the billions—would violate due process.

This case is just one of many that have been filed across the country seeking windfall statutory damages under statutes that are a poor fit for modern technologies like SDKs. Holding Meta liable in this case would not only run counter to the weight of evidence that will be presented at trial, but also harm countless other developers and their users who benefit from tools like the Facebook SDK.

II. FACTUAL BACKGROUND

Software development kits, or SDKs, have multiple components, including different sets of code that correspond to different functionalities. Meta freely and publicly offers certain SDK code, including the Facebook SDK code, for developers to customize to build and improve their apps. Developers choose which SDK code they want, customize it to fit their needs, and integrate it into their apps—all without involvement from Meta. SDKs have become ubiquitous technology, with apps commonly using code from multiple SDKs.

Before using any Facebook SDK code, developers must agree to Meta's Business Tools Terms. Those terms require developers to notify users that they share information with Meta, prohibit developers from sending Meta "health" and other "sensitive" information, and require developers to "have all necessary rights and permissions and a lawful basis to disclose and use" that information. *See, e.g.*, Dkt. 527-3 at 17, 20. Only after agreeing to those terms can a developer incorporate code from the Facebook SDK into its app.

Flo incorporated code from the Facebook SDK and customized it for the Flo App. When users first opened the app, they were prompted to complete an onboarding survey. The survey asked questions such as "When did your last period start?," in response to which users could select a date or say "I don't know." After users responded, the Flo App generated the challenged Custom App Event data. The Custom App Event data were lines of code Flo programmed its app to create that included a name for the Custom App Event and parameter (reflecting binary values, integers, or text values) that corresponded to actions users took within the app. For example, if a user selected "June 12" in response to the question "When did your last period start?," the app would have then created the Custom App Event name "R_SELECT_LAST_PERIOD_DATE" and the parameter "known," *without* any reference to the June 12 date (while the parameter "unknown" would have been sent if a user selected "I don't know"). The Flo App then caused the Event to be stored on the user's device and later

transmitted to Meta's servers, without any information to decode what user action the Event corresponded to. Based on Meta's standard data-retention practices, the underlying Custom App Event data received by Meta from the Flo App was retained for no more than 180 days—meaning it was deleted years before this lawsuit was filed.

Plaintiffs are women who allegedly used the Flo App between November 1, 2016, and February 28, 2019. Plaintiffs all had Facebook accounts during that time, and thus agreed to certain terms and policies, including Meta's Data Policy. Throughout the relevant period, that Policy disclosed that Meta would "collect information when [users] visit[ed] or use[d] third-party websites and apps that use our services," including code from the Facebook SDK. Dkt. 527-3 at 39. The Policy further explained that information collected would "include[] information about the websites and apps you visit" and "information the developer or publisher of the app or website provides to you or [Meta]." *Id.*

Plaintiffs claim that Meta violated CIPA Section 632 because the Flo App sent Meta twelve Custom App Events that allegedly disclosed users' sensitive health information that they entered during the Flo App's onboarding survey. Plaintiffs assert that claim on behalf of a California subclass, defined as "[a]ll Flo App users in California who entered menstruation and/or pregnancy information into the Flo Health App while residing in California" during the class period. Dkt. 605 at 34. Plaintiffs seek statutory "damages for a single violation of CIPA for each member of the California Subclass," or $5,000 per California subclass member. Declaration of Elizabeth McCloskey, Ex. 1 at 5.

III. PLAINTIFFS WILL BE UNABLE TO PROVE THEIR CIPA CLAIM AT TRIAL

To prevail on their only remaining claim against Meta, Plaintiffs must prove that it "intentionally and without the consent of all parties to a confidential communication, use[d] an electronic amplifying or recording device to eavesdrop upon . . . the confidential communication." Cal. Penal Code § 632(a). Plaintiffs will not be able to prove any, much less all, of those elements.

A. Plaintiffs Cannot Prove Meta Eavesdropped On Their Communications

To prevail on their claim against Meta, Plaintiffs must prove it "eavesdropped" on class members' communications with Flo. Cal. Penal Code § 632(a). It is not enough to show that Meta at some point became aware of the substance of such a communication; Plaintiffs have to show that Meta actually listened in on a conversation while it was happening. Or, as the California Supreme Court has

repeatedly put it, there is "a substantial distinction . . . between the secondhand repetition of the contents of a conversation and its simultaneous dissemination to an unannounced second auditor." *E.g.*, *Smith v. LoanMe, Inc.*, 11 Cal. 5th 183, 200 (2021); *Flanagan v. Flanagan*, 27 Cal. 4th 766, 775 (2002). So, if someone were to transcribe a conversation, and then later sends the transcript to a third person, neither the sender nor the recipient would have engaged in "eavesdropping." Here, the evidence will show that the communications Flo sent Meta (the Custom App Events) were not "simultaneous[ly] disseminat[e]d," because they were all sent later than any class members' communications with the Flo App; nor were they even a "secondhand repetition," because none had the same content as class members' communications with the Flo App. *LoanMe*, 11 Cal. 5th at 200.

For example, Defendants' technical expert, Dr. Georgios Zervas, a renowned computer-science expert who has extensive experience working with SDKs, will explain that after a developer decided what Custom App Events to create, its app would create an Event only *after* a user finished performing the action associated with that Event. *See, e.g.*, Dkt. 527-3 at 508, Fig. 2. That Event was then first stored on a user's device before later being sent to Meta. *See id.* Dr. Zervas will detail how the Event was not the same as the information that the user entered into the app. *See* Dkt. 527-3 at 722, Fig. 9. Plaintiffs' own technical expert, Dr. Serge Egelman, agrees: He explained that Flo sent the challenged Custom App Events to Meta only after users finished interacting with the app and after the Events were stored on users' devices. Dr. Egelman also confirmed those Events differed from the information users entered into the app. For example, during the Flo onboarding survey, a user may have selected a period length of three days in response to the question "On average, how long is your period?" But Dr. Egelman's analysis shows that, as a result of that user input, the Flo app code—which included certain code from the SDKs that Flo chose to integrate into its app—generated a separate and distinct set of data: the Event title "R_SELECT_PERIOD_LENGTH" and the parameter "known," without any reference to the three-day duration.

To the extent Plaintiffs' liability theory is that *the SDK itself* eavesdropped on the earlier communications between Plaintiffs and the Flo App, Meta cannot be held liable for eavesdropping under that theory, either. As Dr. Zervas will explain, developers select, modify, and incorporate code from SDKs into their apps, so that the code from the SDKs and an app's code becomes one uniform

set of code. Dr. Egelman agrees the Facebook SDK code does not necessarily send any information at all. The notion that, after this third-party integration process, the "SDK" itself could eavesdrop on communications on Meta's behalf, like some separate piece of spyware, is thus incorrect.

B. Meta Cannot Be Held Liable Because It Was A Party To The Communications

As just discussed, the evidence will show that the only communications Meta received were the Custom App Events that the Flo App sent directly to Meta. But "California courts interpret 'eavesdrop,' as used in § 632, to refer to a third party secretly listening to a conversation between two other parties." *Thomasson v. GC Services Ltd. P'ship*, 321 Fed. App'x 557, 559 (9th Cir. 2008). As a result, Meta cannot be liable under CIPA Section 632 for eavesdropping on the communications the Flo App sent to Meta—because Meta was a party to those communications. *See id.*

C. Plaintiffs Cannot Prove All Parties Did Not Consent

Plaintiffs have the burden to prove Meta eavesdropped on their conversations with the Flo App "without the consent of all parties to the communication[s]." Cal. Penal Code § 632(a). That element forecloses Plaintiffs' claim even if they were parties to the challenged communications, because Plaintiffs and Flo alike consented to the alleged data sharing. All users of Meta's services (e.g., Facebook and Instagram) had to agree to Meta's Data Policy, which disclosed the alleged data sharing. *See supra* at p. 4. And as Facebook users, Plaintiffs agreed to that policy, establishing their consent to Meta's receipt of the information Flo sent. *Smith v. Facebook, Inc.*, 262 F. Supp. 3d 943, 953–55 (N.D. Cal. 2017) (dismissing CIPA claims because plaintiffs consented to the alleged data sharing by agreeing to Meta's Data Policy as Facebook users). The same is true for similarly situated class members. Flo consented by deciding to integrate code from the Facebook SDK, create and name the challenged Custom App Events, and program its app to send that data to Meta. *See* Dkt. 608 at 1 (finding "Flo consented to Meta's data collection practices").

D. Plaintiffs Cannot Prove Any Supposed Eavesdropping Was Intentional

Plaintiffs also must prove that Meta "intentionally" eavesdropped on their and other class members' conversations. Cal. Penal Code § 632(a). To act "intentionally" is to act "consciously and deliberately with the goal" of eavesdropping on their communications with Flo. *United States v. Christensen*, 828 F.3d 763, 791 (9th Cir. 2015). And because Plaintiffs' theory is that Meta

eavesdropped on their "health information," they must prove that Meta intentionally eavesdropped on "the kinds of communications at issue in this lawsuit," i.e., health information. *Doe I v. Google LLC*, 2025 WL 1616720, at *2 (N.D. Cal. June 6, 2025); *see also People v. Super. Ct. of L.A. Cnty.*, 70 Cal. 2d 123, 133 (1969) ("[I]t is not the purpose of the statute to punish a person who intends to make a recording but only a person who intends to make a recording of a confidential communication."); Dkt. 64 ¶¶ 400, 405, 411, 413 (alleging Plaintiffs' "intimate health data . . . was intercepted").

Plaintiffs cannot prove Meta acted with wrongful intent, because the facts will show Meta expressly prohibited Flo from sending it health or other sensitive information. *See supra* p. 3; *see also Doe I*, 2025 WL 1616720, at *2; *B.K. v. Desert Care Networ*k, 2024 WL 1343305, at *7 (C.D. Cal. Feb. 1, 2024) (dismissing CIPA claim against Meta given allegations regarding its "express desire not to receive health data from its business partners"). The facts will also show Meta took steps to mitigate the risk that apps could send data in violation of Meta's policies and terms, including building filters for that information. *See, e.g.*, Dkt. 527-3 at 164–65. The evidence will show that Meta did not want health information and took concrete steps to avoid receiving it.

E. Plaintiffs Cannot Prove Their Communications Were Confidential

Plaintiffs must prove their communications were "confidential"—that is, that they had a "reasonable expectation that the[ir] conversation[s] [were] not being overheard or recorded." *Rodriguez v. Google LLC*, 2021 WL 2026726, at *7 (N.D. Cal. May 21, 2021). Plaintiffs will be unable to do so for three reasons. First, they cannot prove any such "reasonable expectation," because entering information into a period and pregnancy tracking app suggests the information was "by nature recorded" by the app. *Boulton v. Community.com, Inc.*, 2025 WL 314813, at *2 (9th Cir. Jan. 28, 2025). Second, users who had accounts with Meta's services consented to the alleged data sharing by agreeing to Meta's Data Policy, which disclosed that data sharing. *See supra* p. 4. And third, many Plaintiffs willingly shared similar information publicly.

IV. META WILL PREVAIL ON ITS STATUTE-OF-LIMITATIONS DEFENSE

"Under the CIPA, the applicable statute of limitations is one year." *Brodsky v. Apple Inc.*, 445 F. Supp. 3d 110, 134 (N.D. Cal. 2020). To prevail on its statute-of-limitations defense, Meta must prove that the supposed eavesdropping on Plaintiffs happened before June 7, 2020—one year before

they filed this lawsuit against Meta. Meta will prove its receipt of Custom App Events happened before June 7, 2020, because all Plaintiffs testified that they downloaded the Flo App well before that date, and thus went through the onboarding process (during which any of the relevant Custom App Events would have been sent) before that date as well. Their claims are therefore untimely.

To the extent Plaintiffs argue the discovery rule applies, they must prove "(1) the time and manner of discovery and (2) the inability to have made earlier discovery despite reasonable diligence." *Saedi v. SPD Swiss Precision Diagnostics GmbH*, 2025 WL 1141168, at *8 (C.D. Cal. Feb. 27, 2025). "The delayed discovery doctrine only delays accrual until the plaintiff has, or should have, inquiry notice of the cause of action." *Id.* (cleaned up). Inquiry notice refers to "when the plaintiff suspects or should suspect that her injury was caused by wrongdoing." *Id.* at *9. The evidence will show that numerous sources put Plaintiffs on notice of their purported injuries, such as Meta's policies, a February 2019 *Wall Street Journal* article claiming that Flo shared Flo App user data with Meta, and hundreds of news articles published after the *WSJ* article.

V. AWARDING STATUTORY DAMAGES WOULD BE INCONSISTENT WITH THE PURPOSES OF CIPA AND WOULD VIOLATE DUE PROCESS

CIPA provides statutory damages of $5,000 "per violation" of the statute. Cal. Penal Code § 637.2. Plaintiffs want this Court to award statutory damages for "a single violation of CIPA" for each California subclass member—billions of dollars. *See supra* at p. 4. The Court should not do that. For one thing, resolving Plaintiffs' individual claims will not answer all the individualized questions that must be answered before judgment can be entered in favor of the rest of the class. *See infra* at p. 10. For another, even if a jury finds liability, this Court will have discretion to decline to award statutory damages under CIPA. When exercising that discretion, courts "weigh[] several factors, including: (1) the severity of the violation, (2) whether or not there was actual damage to the plaintiff, (3) the extent of any intrusion into the plaintiff's privacy, (4) the relative financial burdens of the parties, (5) whether there was a reasonable purpose for the violation, and (6) whether there is any useful purpose to be served by imposing the statutory damages amount." *Campbell v. Facebook Inc.*, 315 F.R.D. 250, 268 (N.D. Cal. 2016). Plaintiffs will not be able to prove these factors weigh in favor of an award of statutory damages.

Minimal violation and privacy intrusion. The evidence will show that any statutory violation and privacy intrusion would have been minimal given the limited nature of the challenged Custom App Event data and Meta's inability to decipher that data, among other things. For example, Flo did not send Meta anything that would have allowed Meta to understand the meaning of the Custom App Event data. And even if Meta had been given such a key, it would not have yielded much information. Plaintiffs' technical expert agrees that several of the challenged Custom App Events revealed, at most, whether a user responded to an onboarding question, and not the content of that response. Disclosure of that kind of limited data presents minimal, if any, intrusion into any user's privacy.

No actual damage or financial burden. There is no evidence of actual damage to, or financial burden on, any Plaintiff. In their depositions, none of the Plaintiffs identified any quantifiable harm resulting from Meta's receipt of Custom App Events. *See, e.g.*, Dkt. 527-3 at 237.

Reasonable purpose for violation and no useful purpose for award. Plaintiffs will be unable to show Meta had any unreasonable purpose in making SDK code publicly available. As this Court put it, "[t]here is nothing unjust about using an SDK." Dkt. 154 at 10:2-3. Nearly all apps use code from SDKs to improve app functionality and accelerate app development, among other things. And developers chose and customized the code from the Facebook SDK that they wanted to use, subject to Meta's terms. Flo agreed to those terms and was best positioned to ensure its compliance given its direct relationship with its app users and its unique knowledge of the data that it chose to create and send to Meta. Imposing statutory damages on Meta here would not further the statute's purpose, which is to punish affirmative conduct akin to "an eavesdropper pressing up against a door to listen to a conversation." *Licea v. Am. Eagle Outfitters, Inc.*, 659 F. Supp. 3d 1072, 1082 (C.D. Cal. 2023) (cleaned up); Cal. Penal Code § 630.

Awarding anything close to the classwide statutory damages sought here ($5,000 per class member) would also violate due process. Such an award would be "'wholly disproportioned' and 'obviously unreasonable' in relation to the goals of the statute and the conduct the statute prohibits." *Wakefield v. ViSalus, Inc.*, 51 F.4th 1109, 1123–24 (9th Cir. 2022). The Ninth Circuit has recognized that, in cases threatening massive statutory-damages awards, there is a huge gap between the theoretical maximum recovery and what the Constitution permits. In *Wakefield*, for example, the Ninth Circuit

directed the district court to consider whether an aggregate statutory award of $925 million violated due process, noting that, "in the mass communications class action context, vast cumulative damages can be easily incurred" given how "modern technology" functions. 51 F.4th at 1124–25.

VI. EVIDENCE WILL ESTABLISH THERE IS NO BASIS FOR THIS CASE TO PROCEED AS A CLASS ACTION

"A district court may decertify a class at any time," *Rodriguez v. W. Publ'g Corp.*, 563 F.3d 948, 966 (9th Cir. 2009), including after trial and before final judgment, *Mazzei v. Money Store*, 829 F.3d 260, 266 (2d Cir. 2016). The evidence at trial will show that individualized issues do, in fact, "overwhelm common questions and answers." Dkt. 605 at 25. For instance, individualized inquiries are necessary to rule out the significant possibility that a given class member entered fake information into the Flo App and therefore could not have been harmed by that information's supposed disclosure. The evidence will show that many users who went through the onboarding process were just testing out the app and likely entered fake or otherwise non-personal information. *See, e.g.*, Dkt. 490-3 at 1667–68 (identifying circumstances where Custom App Event data is inaccurate, and pointing out that at least 15% of Flo App users identified as "male"). In certifying the class, the Court discounted what it perceived to be "[r]andom anecdotes" of the submission of fake data, Dkt. 605 at 26, but the evidence at trial will show this issue affects a large share of the class.

The evidence will show the same is true for a host of other individualized issues, including, but not limited to, contractual and statutory limitations periods, Article III standing, consent, whether the communications at issue were confidential, whether the communications contained health information, and the factors to be considered when deciding whether to award CIPA statutory damages (as identified in *Campbell*). Against this backdrop, the only way of screening out class members ineligible to recover is through mini-trials incompatible with Rule 23.

Even if the Court declines to decertify the class after trial, Plaintiffs' decision to try this case as a class action cannot deprive Meta of its due-process right to litigate its individualized defenses, and those issues will still need to be adjudicated. *See, e.g.*, *Wal-Mart Stores, Inc. v. Dukes*, 564 U.S. 338, 367 (2011) ("[A] class cannot be certified on the premise that [the defendant] will not be entitled to litigate its statutory defenses to individual claims.").

Dated: June 12, 2025

By: */s/ Andrew B. Clubok*

LATHAM & WATKINS LLP
Andrew B. Clubok (*pro hac vice*)
andrew.clubok@lw.com
555 Eleventh Street NW, Suite 1000
Washington, D.C. 20004
Telephone: 202.637.2200

Melanie M. Blunschi (SBN 234264)
melanie.blunschi@lw.com
Kristin Sheffield-Whitehead (SBN 304635)
kristin.whitehead@lw.com
505 Montgomery Street, Suite 2000
San Francisco, CA 94111-6538
Telephone: 415.395.5942

Michele D. Johnson (SBN 198298)
michele.johnson@lw.com
650 Town Center Drive, 20th Floor
Costa Mesa, CA 92626
Telephone: 714.540.1235

GIBSON, DUNN & CRUTCHER LLP
Elizabeth K. McCloskey (SBN 268184)
EMcCloskey@gibsondunn.com
Abigail A. Barrera (SBN 301746)
ABarrera@gibsondunn.com
One Embarcadero Center, Suite 2600
San Francisco, CA 94111-3715
Telephone: 415.393.8200

Christopher Chorba (SBN 216692)
333 South Grand Avenue
Los Angeles, CA 90071
Telephone: 213.229.7503
CChorba@gibsondunn.com

Counsel for Defendant Meta Platforms, Inc. (formerly known as Facebook, Inc.)

ATTESTATION (CIVIL LOCAL RULE 5-1(i)(3))

In accordance with Civil Local Rule 5-1(i)(3), I attest that concurrence in the filing of this document has been obtained from the signatories.

Dated: June 12, 2025

GIBSON, DUNN & CRUTCHER LLP

/s/ Elizabeth K. McCloskey
Elizabeth K. McCloskey